PlugLink 500 Wireless “N”Adapter

User’s Guide

PL9571-WAP

66-0377-01Rev.001

© 2012 Asoka USA Corporation
ALL RIGHTS RESERVED

Notice: No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of Asoka USA Corporation.

Asoka USA Corporation reserves the right to make changes to this user's guide at any time without notice and assumes no responsibility for its use. Asoka USA products and services can only be ordered under the terms and conditions of Asoka USA Corporation's applicable agreements. All of the features described in this user's guide may not be currently available. Refer to the most recent product announcement for information about feature and product availability.

This user's guide contains the most current information available at the time of publication. When new and/ or revised information becomes available, this entire user's guide is updated and distributed to all registered users.

Asoka, PlugLink, and the Asoka logo are registered trademarks or trademarks of Asoka USA Corporation.

All company and product names mentioned herein are trademarks of their respective companies. Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. Asoka USA Corporation assumes no responsibility with regard to the performance or use of these products.

Revision	Date	Description
66-0377-01Rev.001	July 2012	draft

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR ASOKA REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Asoka's written authorization may result in the equipment no longer complying with FCC requirements for Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference or radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Asoka equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio is on circuits controlled by difference circuit breakers or fuses.)

Modifications to this product not authorized by Asoka could void the FCC approval and negate your authority to operate the product.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. ASOKA DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLED, INCLUDING, WITHOUT LIMITATION, THOSE OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

IN THE EVENT SHALL ASOKA BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF INABILITY TO USE THIS MANUAL, EVEN IF ASOKA HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Contact Information

For more information about the PlugLink 500 Wireless "N" Adapter or any of Asoka's other leading-edge solutions, please contact us using any of the following methods:

- **Voice calls**: (408) 550-8167 - We welcome your calls Monday through Friday, from 9:00 am to 5:00 pm Pacific Time. Voice mail is available during non-business hours.
- **Email**: If you prefer, you can send information requests to our e-mail address: sales@asokatech.com.
- **Web site**: Our Web site contains valuable information about our products, solutions, and services. We encourage you to visit us at http://www.asokatech.com.

Customer Service

Available from: Monday through Friday, from 9:00 am to 5:00 pm Pacific Time, by calling (408) 550-8167 or through email at custserv@asokatech.com.

Technical Support

Technical support is available Monday through Friday, from 8:00 am to 5:00 pm Pacific Time, by calling (408) 550-8173 or through email at support@asokatech.com.

Please provide the following information about the problem:

- Product name and model.
- System configuration, including a description of the devices connected to your PlugLink 500 Wireless "N" Adapter.
- The circumstances surrounding the error or failure.
- A detailed description of the problem and what has been done to try to solve it.

Table of Contents

Chapter 1 3
Introduction 3
Chapter 2 4
Important Safety Instruction 4
Chapter 3 5
Learning about PL9571 5
Chapter 4 8
Preparing to Install 8
Chapter 5 9
Installing PL9571 9
Chapter 6 11
Logging on 11
Chapter 7 13
Basic Configuration 13
Chapter 8 20
Advanced Configuration 20
Chapter 9 33
Technical Support 33
Chapter 10 34
Technical Specification 34
Chapter 11 33
FCC Statement 35
Chapter 12 34
Warranty Information 36

Chapter 1

Introduction

Thank you for purchasing a PlugLink 500 Wireless "N" Adapter from Asoka. This adapter lets you extend an existing Powerline network allowing you to set up an instant wireless hotspot simply by plugging into a power outlet. With your PlugLink 500 Wireless "N" Adapter, you can easily share your high-speed Internet broadband, mp3s, video and gaming throughout the home or home office without pulling any new cabling.

This unit will not interfere with other household appliances such as hair dryers, vacuum cleaners or microwave ovens. Consuming only 7 watts of power, it is environmentally friendly and will not noticeably increase your electrical bill. It is a simple, secure and reliable choice for web surfing, playing games, and complimenting your existing wireless network, mp3 streaming and even video sharing.

This User's Guide shows you how to connect your PlugLink 500 Wireless "N" Adapter to your existing Powerline network. Setup is easy. Just follow the instructions in this guide, your network will be up and running in a matter of minutes.

Chapter 2

Important Safety Instruction

The following precautions should be taken when using this product:

- Read all instructions before installing and operating this product.
- Do not open the cover or casing on this product and/or alter this product in any way.
- Follow common household electrical safety practices.

If you have any questions or concerns regarding these safety measures, please contact Technical Support via email at support@asokatech.com or via phone at 408-550-8173 Monday through Friday between 9:00 am and 5:00 pm PST (excluding holidays.

Chapter 3

Learning about PL9571

Package Contents
- PlugLink 500 Wireless “N” Adapter (PL9571-WAP)
- Quick Installation Guide
- Installation Resource CD
- Warranty and Support Information Card
- Ethernet Cable

IF ANY OF THE PARTS ARE INCORRECT, MISSING, OR DAMAGED, CONTACT THE RETAILER WHERE OU MADE YOUR PURCHASE. Keep the carton, including the original packing materials, in case you need to return the unit for repair.

The Front Panel

The front panel of the PL9571-WAP Adapter contains the status lights described below.

Figure 3-1: PL9571-WAP Front Panel

You can use the status lights to verify connections. Viewed from top to bottom, left to right, the table describes the lights on the front panel of the unit.

Table 3-1: Status Light Descriptions

Power	On	Indicates Device Powered On
	Off	Indicates No Power
PLC Activity	Blinking. The colors act as throughput indicators.	Indicates Activity on Powerline. Green means good throughput. Orange means average throughput
	Off	Indicates No Activity on Powerline (Should blink Intermittently)
Wireless Activity	Blinking	Indicates Activity on Wireless
	Off	Indicates No Activity on Wireless
ETH Link	On	Indicates Ethernet Connectivity
	Blinking	Indicates Ethernet Traffic Indicates
	Off	No Ethernet Activity

The Bottom Panel

The bottom panel of the PL9571-WAP two (RJ-45) ports shown in figure 3-2.

- *Figure 3-2: PL9571-WAP Bottom Panel*

The Rear Panel

The label on the rear panel of the PL9571-WAP Adapter contains the items listed below.

Model number
Unique device password
PLC MAC Address
Device MAC Address
Serial number

Note: For future convenience, please write this information down in your Warranty and Support Information Card.

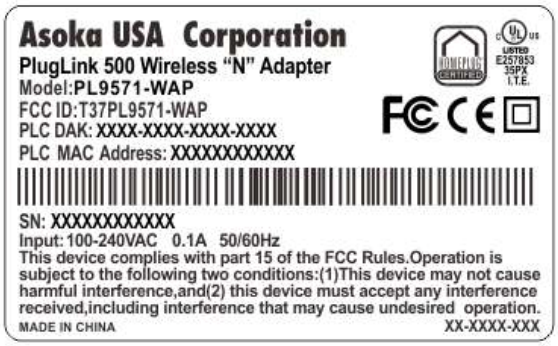

Asoka USA Corporation
PlugLink 500 Wireless "N" Adapter
Model:PL9571-WAP
FCC ID:T37PL9571-WAP
PLC DAK: XXXX-XXXX-XXXX-XXXX
PLC MAC Address: XXXXXXXXXXXX
SN: XXXXXXXXXXXX
Input: 100-240VAC 0.1A 50/60Hz
This device complies with part 15 of the FCC Rules.Operation is subject to the following two conditions:(1)This device may not cause harmful interference,and(2) this device must accept any interference received,including interference that may cause undesired operation.
MADE IN CHINA
XX-XXXX-XXX

Figure 3-3: Rear Label

Buttons

The PlugLink 500 Wireless "N" Adapter device has three push buttons:

SW1 (Left) Button / Powerline Security - The **NID** button allows you to set a randomized Network Encryption Key (NEK) by pressing it. You can then have additional units use the same randomized NEK by pressing their respective **NID** buttons.

SW2 (Front) Button / WPS Wireless and power- Key reuse, and the button at different times, said two functions.

1. This button allows you to configure wireless security by simply pushing a button. This requires software and a network adapter that supports this feature.
2. This button allows you to configure wireless power.

SW3– Resets the PlugLinK9571 back to factory default settings. Press and hold the button with a pin or sharp object for about 2 seconds until you see the lights on the device flash briefly.

Chapter 4

Preparing to Install

The PlugLink 500 Wireless "N" Adapter lets you set up an instant wireless Access Point using your existing electrical outlets. It can also easily compliment your existing network by connecting to any device with a 10/100BaseT Ethernet-capable device.

To setup a PLC (PowerLine Communication) Network you will need:

- One (1) PL9571-WAP device
- One (1) PL9660-Q1 device (sold separately)
- Standard Cable/ DSL gateway (provided by your ISP)

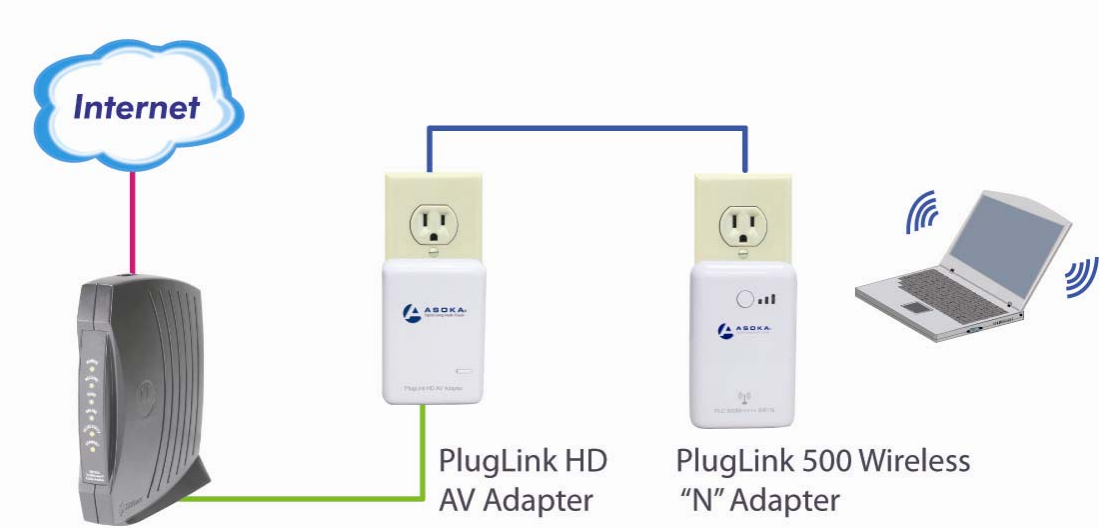


Figure 4-1: Connecting PL9571-WAP with PL9661-ETH diagram

Chapter 5

Installing PL9571

Note

Do not connect the PlugLink 500 Wireless “N” Adapter to a power strip, extension cord, uninterruptible power supply (UPS), or surge protector. This may prevent the unit from working property or degrade the network performance.

Plug the PlugLink 500 Wireless “N” Adapter into the wall outlet vertically (right side up).

1. Use the Ethernet cable shipped with your PlugLink HD AV Adapter PL9660-Q1 (PL9660-Q1 not included; sold separately) to a LAN port on your router.

2. Plug the PlugLink HD AV Adapter PL9660 (PL9660-Q1 not included) into a nearby wall outlet.

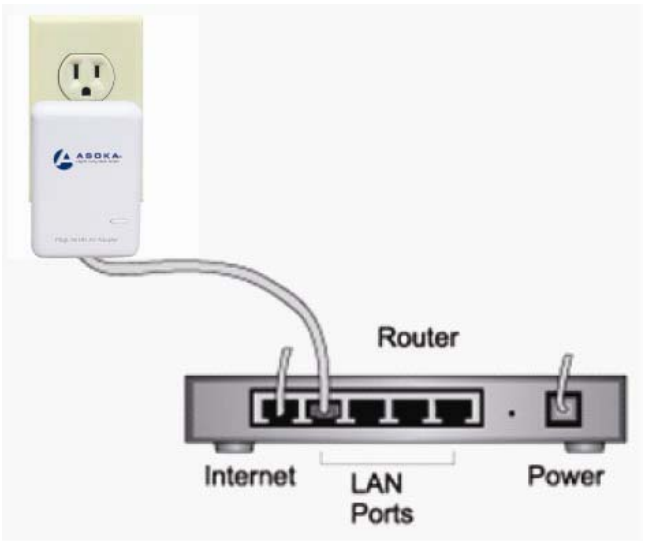


Figure 5-1: Connecting the PL9661-ETH to a router.

3. Plug the PlugLink 500 Wireless “N” Adapter into a wall outlet near the wireless computer that you want to connect.

Figure 5-2: Plugging the PL9571-WAP vertically into a wall outlet.

4. Wait a few seconds and the top three LEDs on the PlugLink 500 Wireless “N” Adapter will light up.
5. From your computer scan your Wireless Network Connections to look for your PlugLink 500 Wireless “N” Adapter’s network name (SSID). The default name (SSID) of the PlugLink 500 Wireless “N” Adapter is **Asoka**. You will be prompted for your “Encryption Key”. The default Encryption Key is the last 10 digits of the serial number. The serial number is printed on the PL9571 label.

Note	If you changed the default network name (SSID), be sure to use the correct network name (SSID) you set in the PlugLink 500 Wireless “N” Adapter.

Note	Wireless security is enabled by default on the PL9571-WAP. For more information about changing the PL9571-WAP security settings, see the subsection in Chapter 10 entitled *Wireless Security*.

6. Verify wireless connectivity by connecting to the Internet or log into the PL9571-WAP from a computer with a wireless adapter.

Chapter 6

Logging on

1. Open a web browser application (Internet Explorer or Mozilla Firefox).
2. Enter the router's default IP address (*192.168.1.254*) in the URL address field. Press **Enter** to open the login screen..

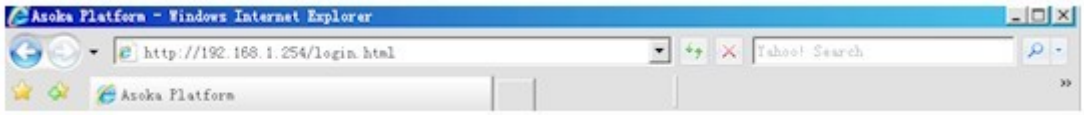


Figure 6-1: Login Address

For security, the PL9571-WAP has its own user ID and password. When prompted, enter admin for the user ID, welcome for the password, both in lower case letters, and press Login. To change the login password, see "Setting or Changing the Administrative Login Information" on chapter 10.

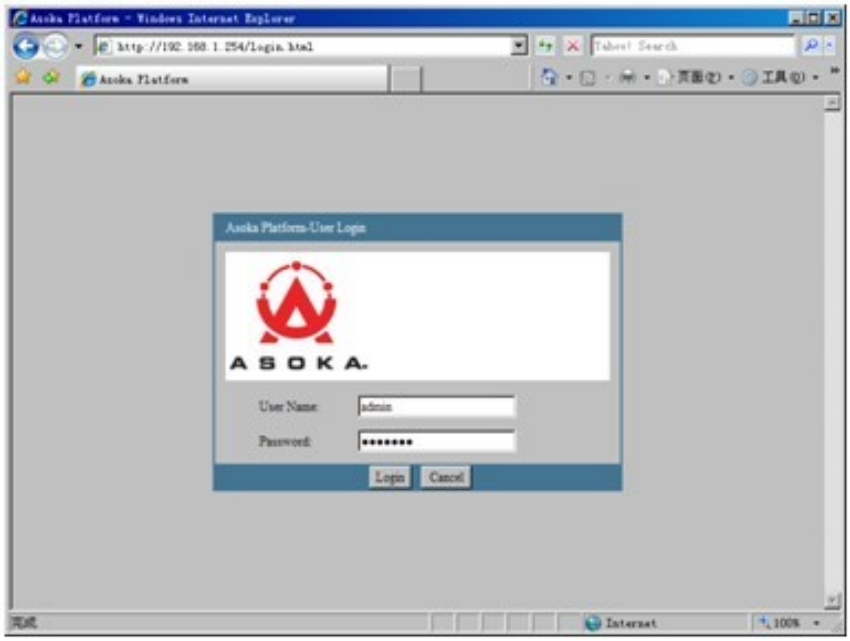
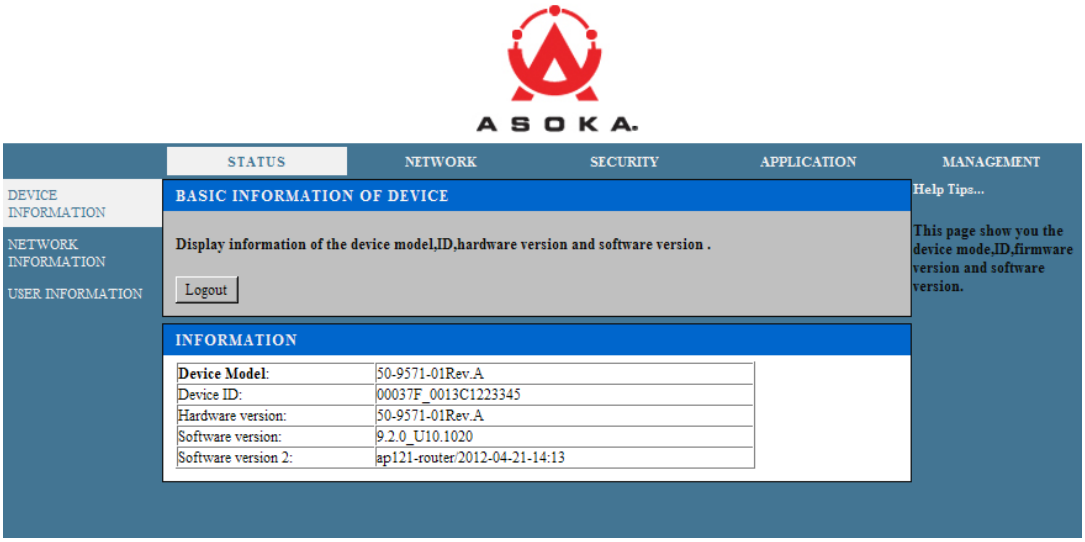


Figure 6-2: Login Screen

3. The first time the login screen opens, use the default user name admin and password welcome. Click **Login (**Note that user accounts are managed in User Account Management and can be changed after the first login.)

The web interface opens to the basic devices information.



Chapter 7

Basic Configuration

Working mode
Middleware-enabled platforms have two operation modes:

To configure AP mode using the router (router build only):
1. Choose the **NETWORK** tab to open the Network Connection Settings:
2. Select *Enable Access Point Mode*. A confirmation box appears. Click **OK**.
3. A confirmation screen appears. The router will now work in AP mode.

To configure router mode using the AP:

Unselect the check box Enable Access Point Mode.
Router Build Software that is built with **BUILD_CONFIG=-router** in the build process (user scan select between full router mode and AP mode)
AP Build Software not built using **BUILD_CONFIG=-router**. For AP build, *Enable AP Mode* is selected automatically and grayed out; users cannot change modes

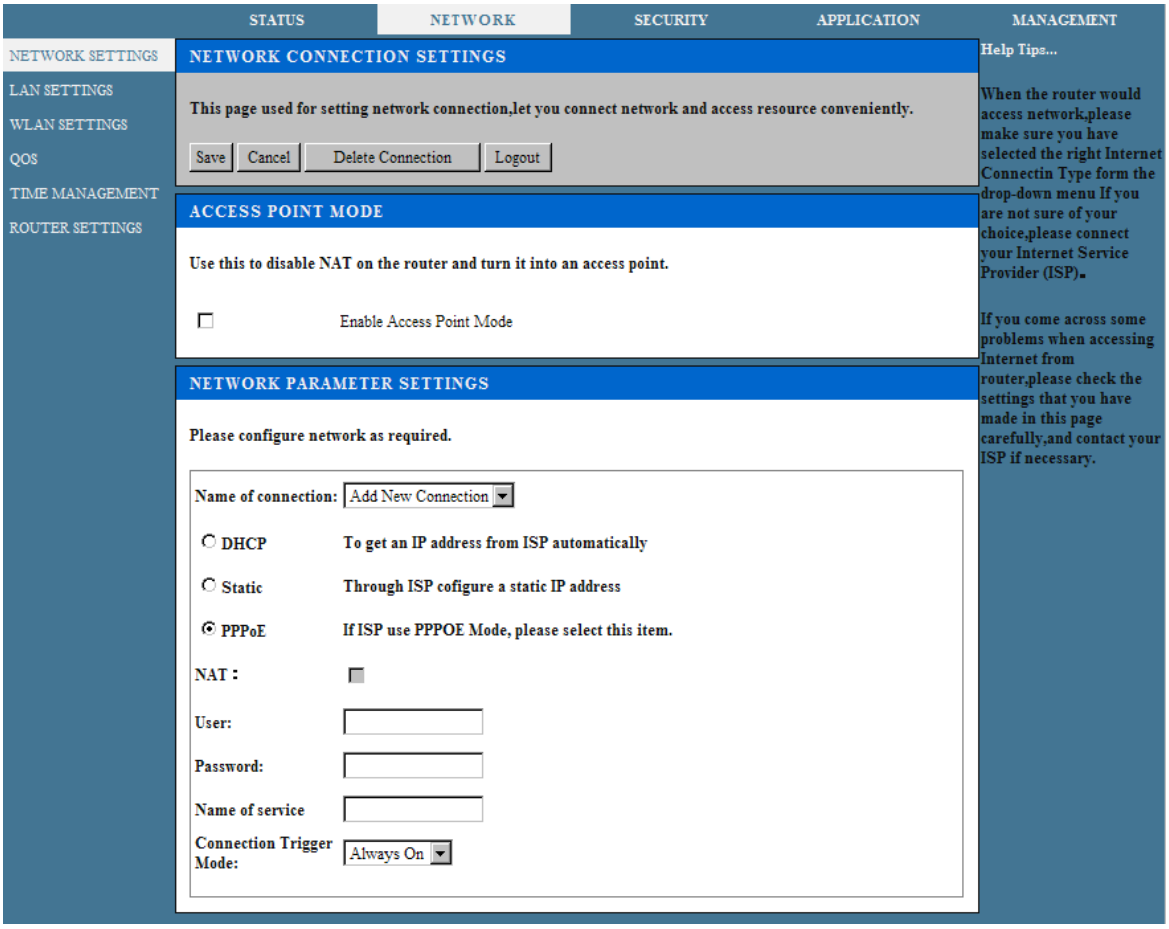
ASOKA
STATUS
NETWORK
SECURITY
APPLICATION
MANAGEMENT
NETWORK SETTINGS
LAN SETTINGS
WLAN SETTINGS
QOS
TIME MANAGEMENT
ROUTER SETTINGS
NETWORK CONNECTION SETTINGS
This page used for setting network connection,let you connect network and access resource conveniently.
Save
Cancel
Delete Connection
Logout
ACCESS POINT MODE
Use this to disable NAT on the router and turn it into an access point.
Enable Access Point Mode
Help Tips...
When the router would access network,please make sure you have selected the right Internet Connectin Type form the drop-down menu If you are not sure of your choice,please connect your Internet Service Provider (ISP).
If you come across some problems when accessing Internet from router,please check the settings that you have made in this page carefully,and contact your ISP if necessary.

Select *Enable Access Point Mode*. A confirmation box appears. Click **OK**.

A confirmation screen appear, the router will now work in Router Mode.
To configure router mode using the Ap: unselect the check box Enable Access Point Mode.

To add a PPPoE internet connection:
See "To set the router IP address" on page 24 for how to configure the router to the Internet connection. Much of this information is obtained from the ISP.

1. Choose the **NETWORK** tab to open the Network Connection Settings:

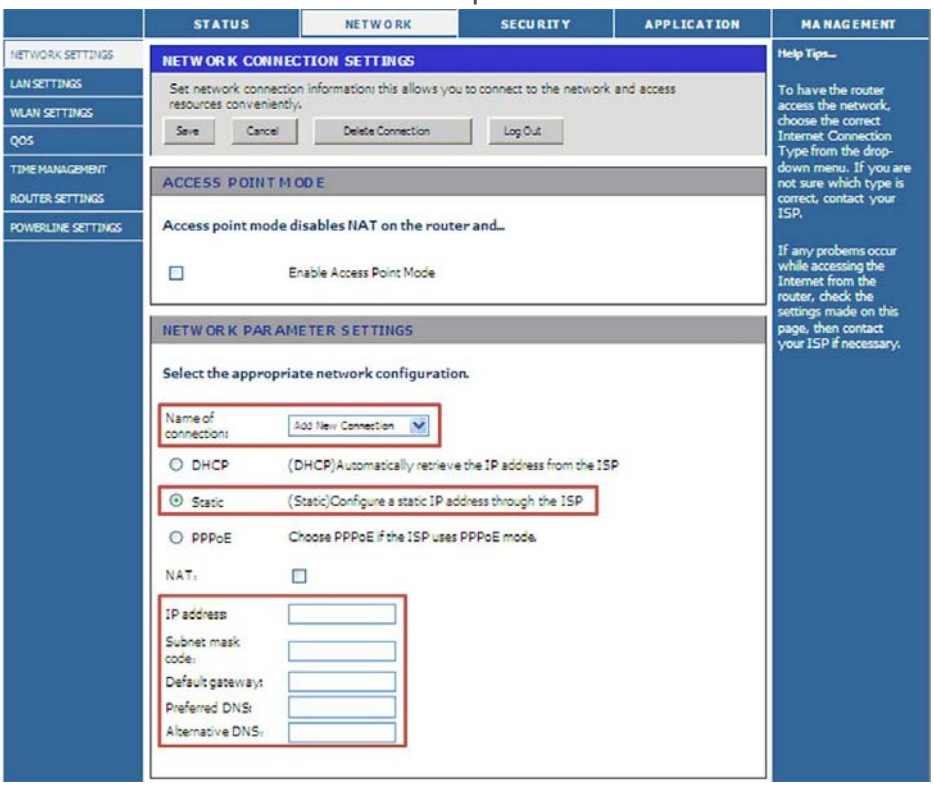

STATUS
NETWORK
SECURITY
APPLICATION
MANAGEMENT
NETWORK SETTINGS
LAN SETTINGS
WLAN SETTINGS
QOS
TIME MANAGEMENT
ROUTER SETTINGS
NETWORK CONNECTION SETTINGS
This page used for setting network connection,let you connect network and access resource conveniently.
Save
Cancel
Delete Connection
Logout
ACCESS POINT MODE
Use this to disable NAT on the router and turn it into an access point.
Enable Access Point Mode
NETWORK PARAMETER SETTINGS
Please configure network as required.
Name of connection:
Add New Connection
DHCP
To get an IP address from ISP automatically
Static
Through ISP cofigure a static IP address
PPPoE
If ISP use PPPOE Mode, please select this item.
NAT :
User:
Password:
Name of service
Connection Trigger Mode:
Always On
Help Tips...
When the router would access network,please make sure you have selected the right Internet Connectin Type form the drop-down menu If you are not sure of your choice,please connect your Internet Service Provider (ISP).
If you come across some problems when accessing Internet from router,please check the settings that you have made in this page carefully,and contact your ISP if necessary.

2. At *Name of Connection*, make sure *Choose New Connection* is selected.
3. Select the connection type *PPPoE*.

4. Enter the user name and password provided by the ISP. Leave *Name of Service* blank if unsure.
5. Select the preferred dial-up style under *Dial-up Method*.
6. Click **Save** to commit the changes.

To add a DHCP internet connection:

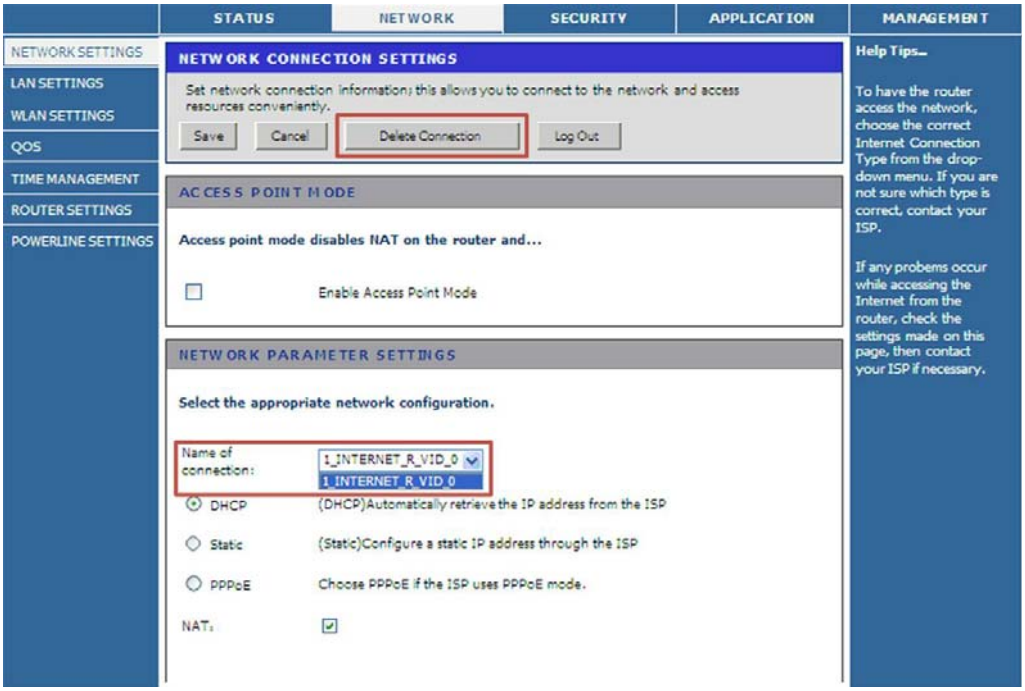
1. Choose the **NETWORK** tab to open the Network Connection Settings:


STATUS
NETWORK
SECURITY
APPLICATION
MANAGEMENT
NETWORK SETTINGS
LAN SETTINGS
WLAN SETTINGS
QOS
TIME MANAGEMENT
ROUTER SETTINGS
POWERLINE SETTINGS
NETWORK CONNECTION SETTINGS
Set network connection information this allows you to connect to the network and access resources conveniently.
Save
Cancel
Delete Connection
Log Out
ACCESS POINT MODE
Access point mode disables NAT on the router and...
Enable Access Point Mode
NETWORK PARAMETER SETTINGS
Select the appropriate network configuration.
Name of connection:
Add New Connection
DHCP
(DHCP)Automatically retrieve the IP address from the ISP
Static
(Static)Configure a static IP address through the ISP
PPPoE
Choose PPPoE if the ISP uses PPPoE mode.
NAT:
IP address:
Subnet mask code:
Default gateway:
Preferred DNS:
Alternative DNS:
Help Tips...
To have the router access the network, choose the correct Internet Connection Type from the drop-down menu. If you are not sure which type is correct, contact your ISP.
If any problems occur while accessing the Internet from the router, check the settings made on this page, then contact your ISP if necessary.

2. At *Name of Connection*, make sure *Choose New Connection* is selected.
3. Select the connection type *Static*.
4. Fill in the boxes for:
   IP Address
   Subnet mask code
   Default gateway
   Preferred DNS
   Alternative DNS (optional)
5. Click **Save** to commit the changes

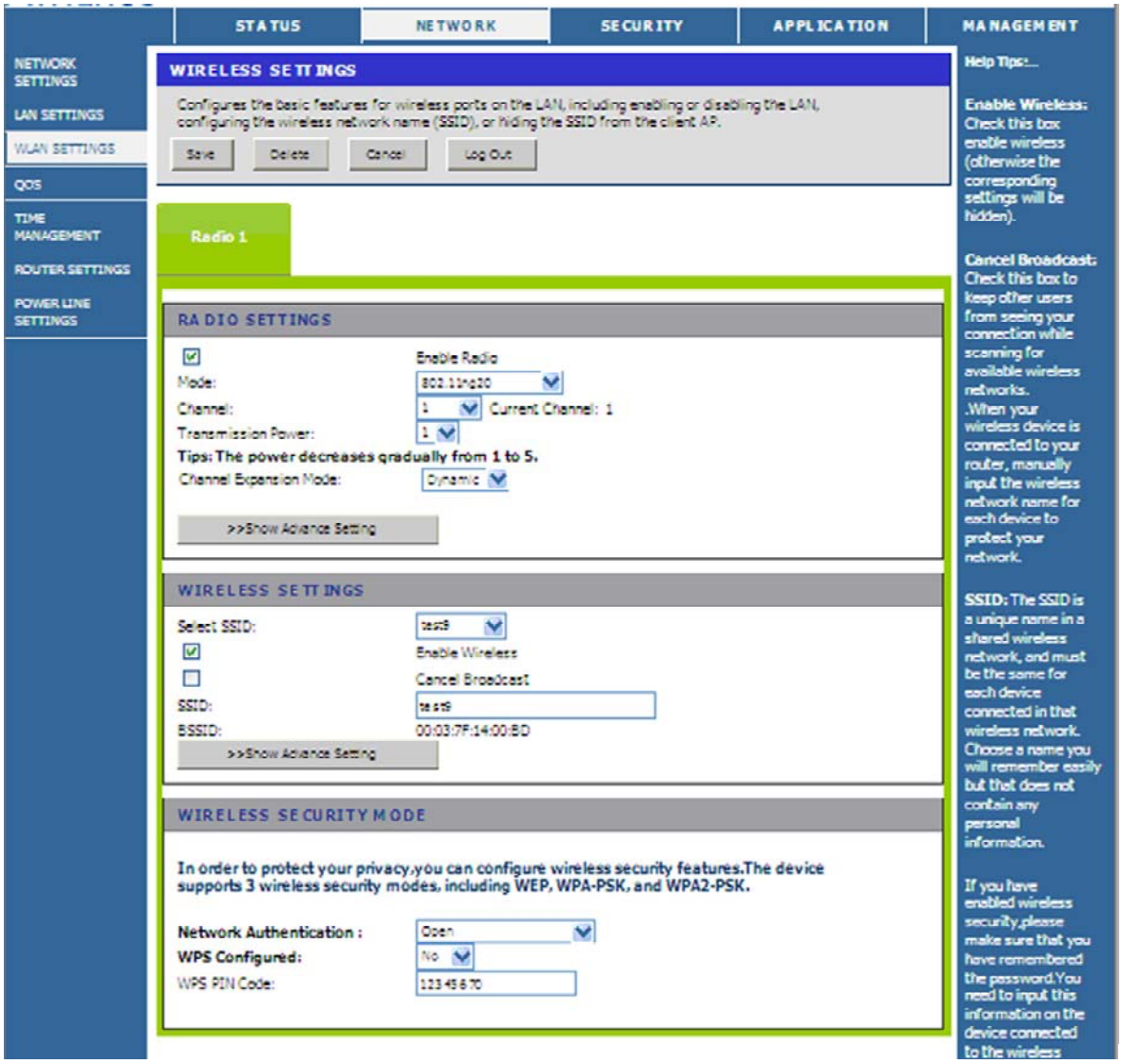
To delete an internet connection:

1. Choose the NETWORK tab to open the Network Connection Settings.
2. At Name of Connection, choose the name of the connection to delete.
3. Click Delete Connection.


STATUS
NETWORK
SECURITY
APPLICATION
MANAGEMENT
NETWORK SETTINGS
LAN SETTINGS
WLAN SETTINGS
QOS
TIME MANAGEMENT
ROUTER SETTINGS
POWERLINE SETTINGS
NETWORK CONNECTION SETTINGS
Set network connection information; this allows you to connect to the network and access resources conveniently.
Save
Cancel
Delete Connection
Log Out
ACCESS POINT MODE
Access point mode disables NAT on the router and...
Enable Access Point Mode
NETWORK PARAMETER SETTINGS
Select the appropriate network configuration.
Name of connection:
1_INTERNET_R_VID_0
1_INTERNET_R_VID_0
DHCP
(DHCP)Automatically retrieve the IP address from the ISP
Static
(Static)Configure a static IP address through the ISP
PPPoE
Choose PPPoE if the ISP uses PPPoE mode.
NAT:
Help Tips...
To have the router access the network, choose the correct Internet Connection Type from the drop-down menu. If you are not sure which type is correct, contact your ISP.
If any probems occur while accessing the Internet from the router, check the settings made on this page, then contact your ISP if necessary.

Wireless LAN (WLAN) Setup

Set up a WLAN either manually or by using WiFi protected setup (WPS). WPS allows easy setup of client devices that support WPS. Choose the **NETWORK** tab, then choose the **WLAN SETTINGS** tab to open the Radio Settings screen. Note that WPS configures one client device at a time. Repeat the instructions for each client device that supports WPS.


STATUS
NETWORK
SECURITY
APPLICATION
MANAGEMENT
NETWORK SETTINGS
LAN SETTINGS
WLAN SETTINGS
QOS
TIME MANAGEMENT
ROUTER SETTINGS
POWER LINE SETTINGS
WIRELESS SETTINGS
Configures the basic features for wireless ports on the LAN, including enabling or disabling the LAN, configuring the wireless network name (SSID), or hiding the SSID from the client AP.
Save
Delete
Cancel
Log Out
Radio 1
RADIO SETTINGS
Enable Radio
Mode:
Channel:
Current Channel: 1
Transmission Power:
Tips: The power decreases gradually from 1 to 5.
Channel Expansion Mode:
Dynamic
>>Show Advance Setting
WIRELESS SETTINGS
Select SSID:
Enable Wireless
Cancel Broadcast
SSID:
BSSID:
00:03:7F:14:00:BD
>>Show Advance Setting
WIRELESS SECURITY MODE
In order to protect your privacy,you can configure wireless security features.The device supports 3 wireless security modes, including WEP, WPA-PSK, and WPA2-PSK.
Network Authentication :
Open
WPS Configured:
No
WPS PIN Code:
12345670
Help Tips:...
Enable Wireless: Check this box enable wireless (otherwise the corresponding settings will be hidden).
Cancel Broadcast: Check this box to keep other users from seeing your connection while scanning for available wireless networks. .When your wireless device is connected to your router, manually input the wireless network name for each device to protect your network.
SSID: The SSID is a unique name in a shared wireless network, and must be the same for each device connected in that wireless network. Choose a name you will remember easily but that does not contain any personal information.
If you have enabled wireless security,please make sure that you have remembered the password.You need to input this information on the device connected to the wireless

Figrure7-2 WPS Setup Screen

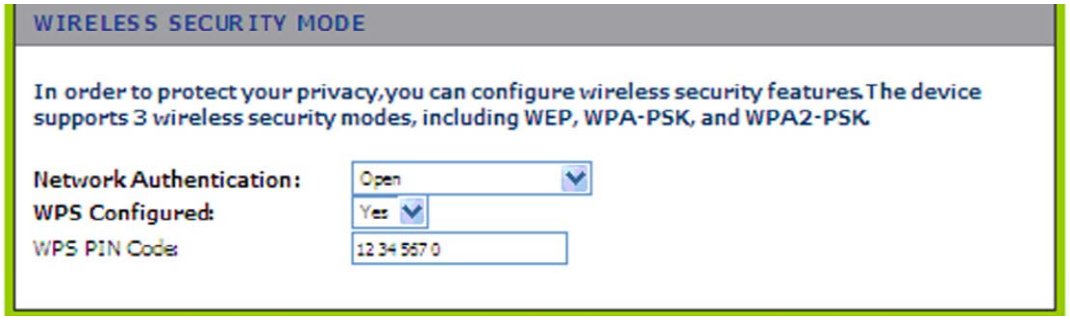
To user automatic automatic WPS configuration:

1. Under the Wireless Security Mode section of the WPS setup screen:

In the WPS Configured drop-down menu, choose Yes.

For a client device with a WPS button: click the WPS button on the client device, then click the WPS button on the router board. After the client device has been configured, click OK. See the client device documentation for more instructions.

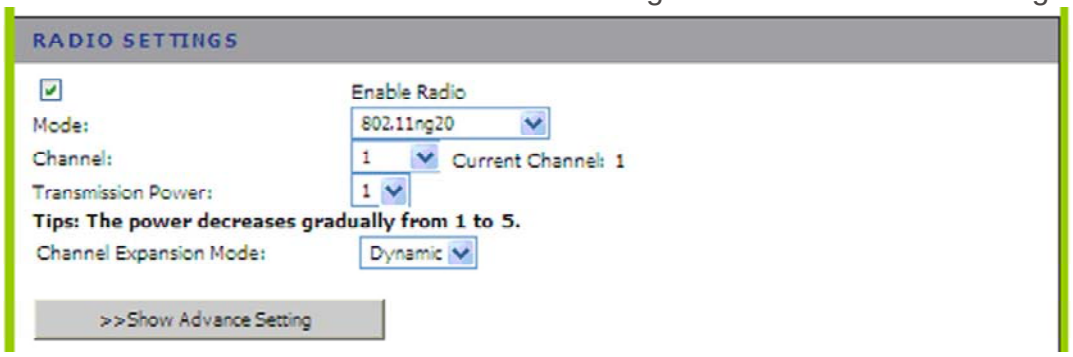
For a client device that asks for a Router PIN number: enter the PIN number listed on the web page (or on the label on the bottom of the router). After the client device has been configured, click OK. See the client device documentation for more instructions.


WIRELESS SECURITY MODE
In order to protect your privacy,you can configure wireless security features.The device supports 3 wireless security modes, including WEP, WPA-PSK, and WPA2-PSK.
Network Authentication:
Open
WPS Configured:
Yes
WPS PIN Code:
12 34 567 0

2. Click Save to commit the changes.

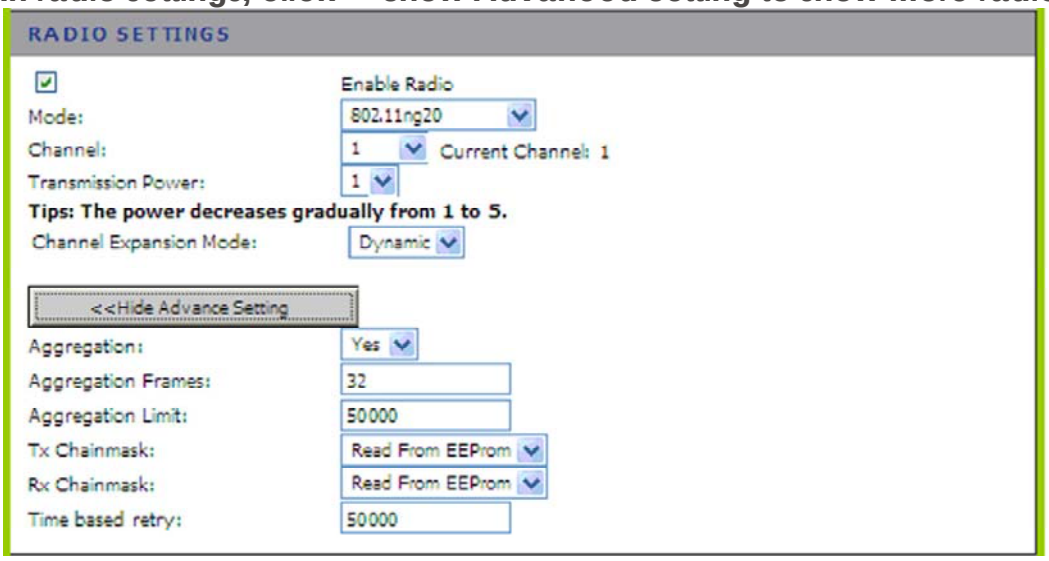
To use manual WLAN configuration:

1. Enable the radio under the radio settings section of WLAN settings:

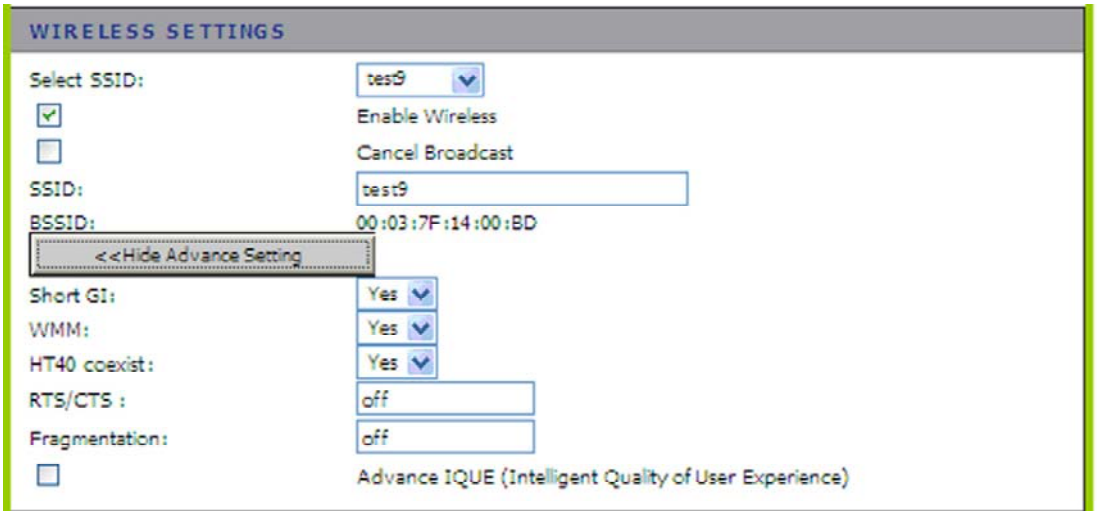


2. Select the mode, channel, and transmission power levels.
3. Click **Save** to commit the changes.

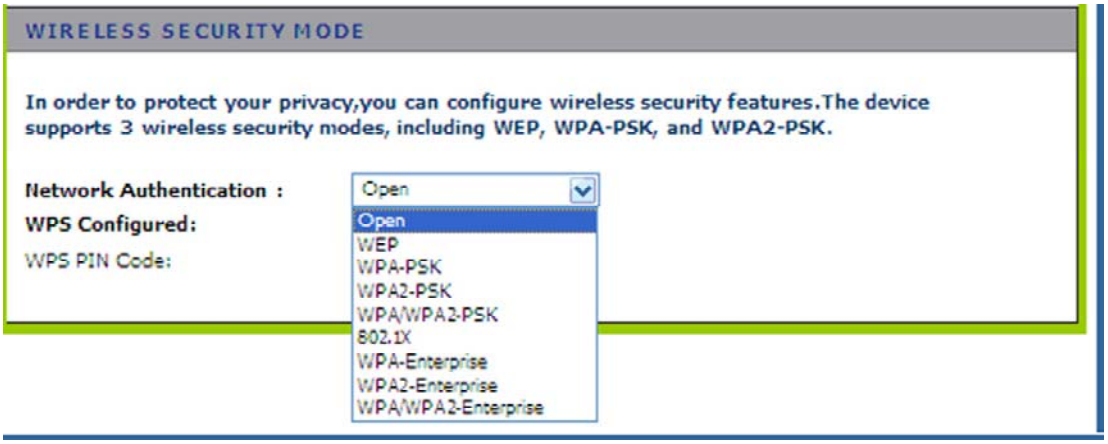
In radio settings, click >>Show Advanced Setting to show more radio settings:



View the basic wireless settings on the wireless settings screen. Click >>Show Advanced Setting to show more wireless settings:



View the wireless security mode settings on the WLAN settings screen:

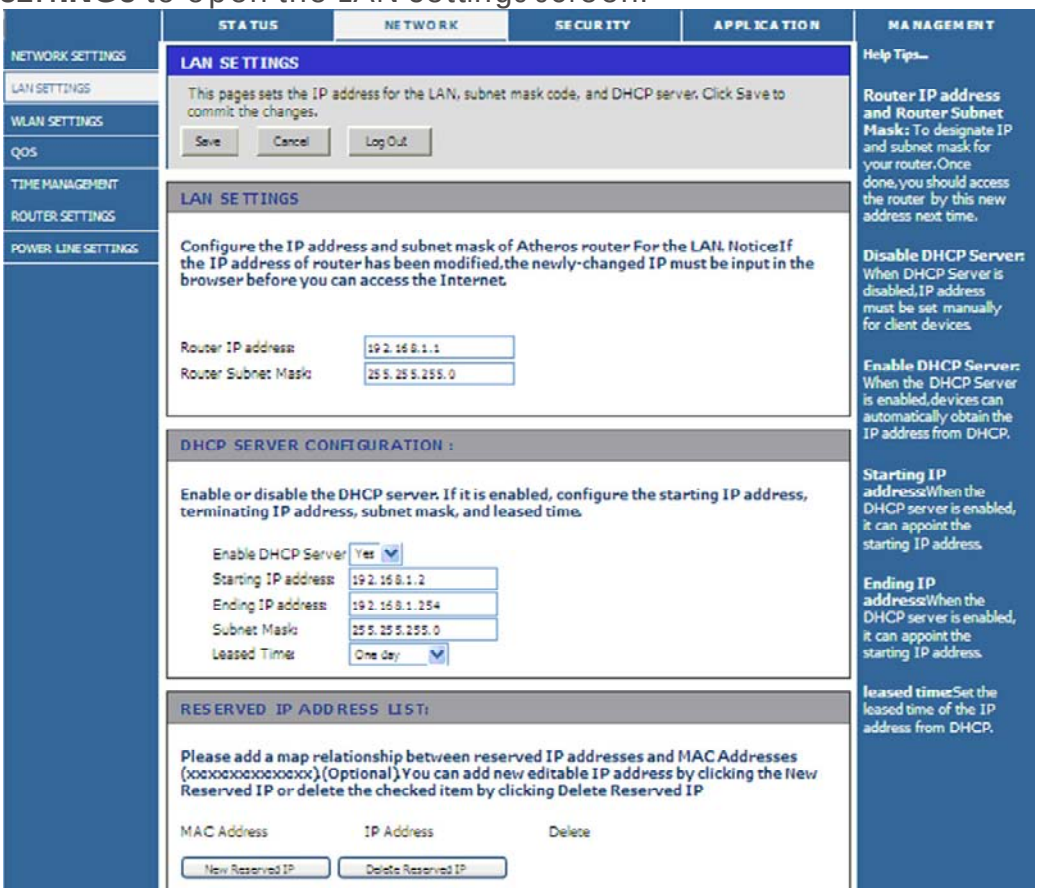


Chapter 8

Advanced Configuration

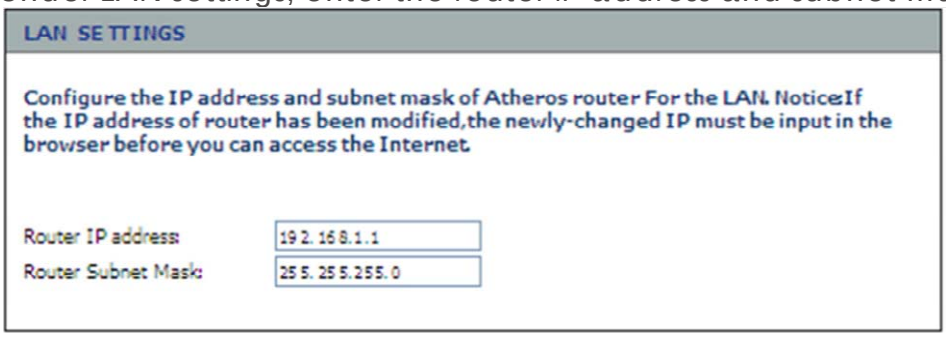
3.2.1 Local Area Network (LAN) Settings

Choose the **NETWORK** tab to open the Network Connection Settings, **LAN SETTINGS** to open the LAN Settings screen:


STATUS
NETWORK
SECURITY
APPLICATION
MANAGEMENT
NETWORK SETTINGS
LAN SETTINGS
WLAN SETTINGS
QOS
TIME MANAGEMENT
ROUTER SETTINGS
POWER LINE SETTINGS
LAN SETTINGS
This pages sets the IP address for the LAN, subnet mask code, and DHCP server. Click Save to commit the changes.
Save
Cancel
Log Out
LAN SETTINGS
Configure the IP address and subnet mask of Atheros router For the LAN. Notice:If the IP address of router has been modified,the newly-changed IP must be input in the browser before you can access the Internet.
Router IP address:
192.168.1.1
Router Subnet Mask:
255.255.255.0
DHCP SERVER CONFIGURATION :
Enable or disable the DHCP server. If it is enabled, configure the starting IP address, terminating IP address, subnet mask, and leased time.
Enable DHCP Server
Yes
Starting IP address:
192.168.1.2
Ending IP address:
192.168.1.254
Subnet Mask:
255.255.255.0
Leased Time:
One day
RESERVED IP ADDRESS LIST:
Please add a map relationship between reserved IP addresses and MAC Addresses (xxxxxxxxxxxx).(Optional).You can add new editable IP address by clicking the New Reserved IP or delete the checked item by clicking Delete Reserved IP
MAC Address
IP Address
Delete
New Reserved IP
Delete Reserved IP
Help Tips...
Router IP address and Router Subnet Mask: To designate IP and subnet mask for your router.Once done,you should access the router by this new address next time.
Disable DHCP Server: When DHCP Server is disabled,IP address must be set manually for client devices.
Enable DHCP Server: When the DHCP Server is enabled,devices can automatically obtain the IP address from DHCP.
Starting IP address:When the DHCP server is enabled, it can appoint the starting IP address.
Ending IP address:When the DHCP server is enabled, it can appoint the starting IP address.
leased time:Set the leased time of the IP address from DHCP.

To set the router IP address

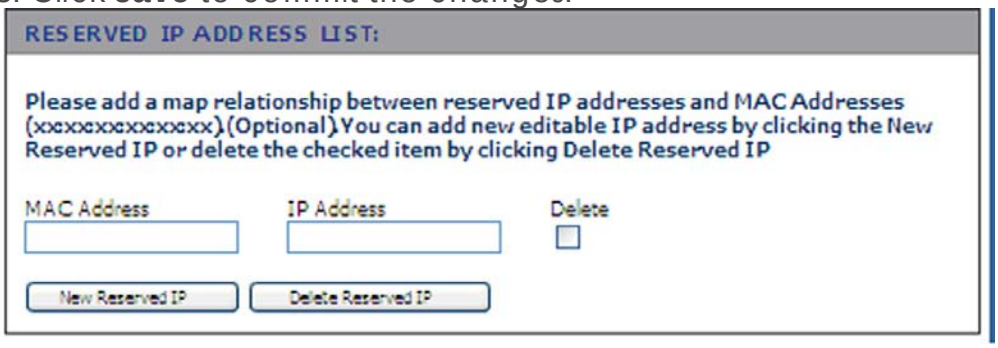
1. Under LAN settings, enter the router IP address and subnet mask.


LAN SETTINGS
Configure the IP address and subnet mask of Atheros router For the LAN. Notice:If the IP address of router has been modified,the newly-changed IP must be input in the browser before you can access the Internet.
Router IP address:
192.168.1.1
Router Subnet Mask:
255.255.255.0

2. Click **Save** to commit the changes.

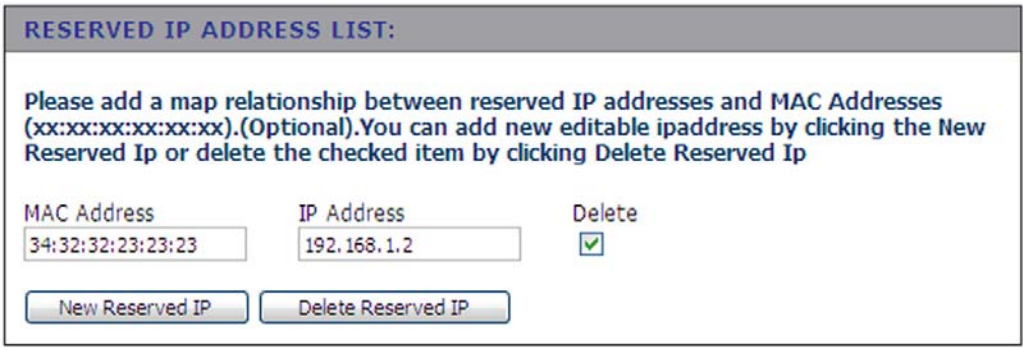
To set the IP address reserve (router build only):

1. Under Reserved IP Address List, click **New Reserved IP**:
2. Fill in the MAC address and IP address.
3. Click **Save** to commit the changes.


RESERVED IP ADDRESS LIST:
Please add a map relationship between reserved IP addresses and MAC Addresses (xxxxxxxxxxxx).(Optional).You can add new editable IP address by clicking the New Reserved IP or delete the checked item by clicking Delete Reserved IP
MAC Address
IP Address
Delete
New Reserved IP
Delete Reserved IP

To delete a reserved IP:

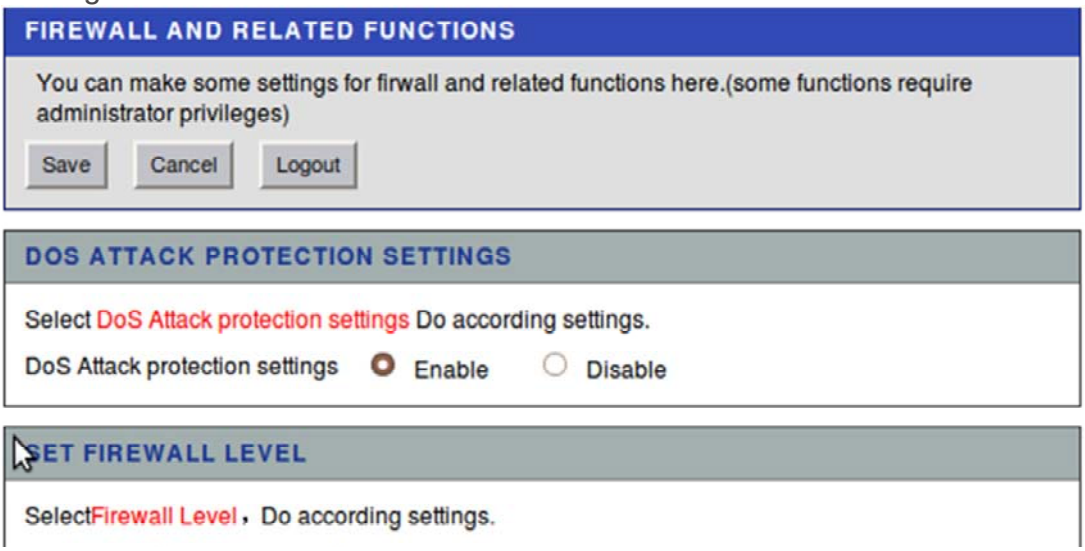
1. Under Reserved IP Address List, click **Delete Reserved IP**:.


RESERVED IP ADDRESS LIST:
Please add a map relationship between reserved IP addresses and MAC Addresses (xx:xx:xx:xx:xx:xx).(Optional).You can add new editable ipaddress by clicking the New Reserved Ip or delete the checked item by clicking Delete Reserved Ip
MAC Address
IP Address
Delete
34:32:32:23:23:23
192.168.1.2
New Reserved IP
Delete Reserved IP

2. Check the Delete box next to the address to delete.
3. Click **Delete Reserved IP** button.

3.2.2 Firewall (Router Build Only)

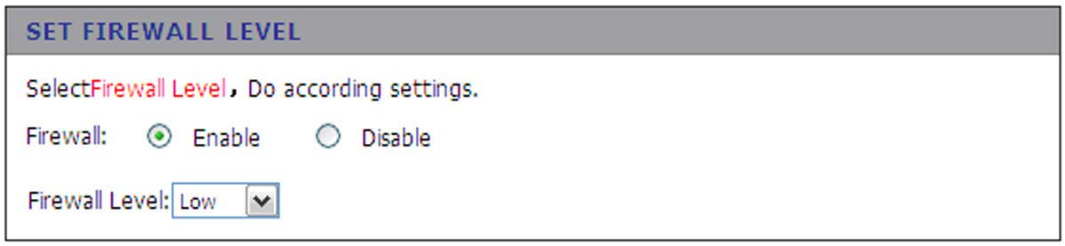
Choose the **SECURITY** tab to open the LAN Settings, then click **FIREWALL** on the LAN
Settings screen:


FIREWALL AND RELATED FUNCTIONS
You can make some settings for firwall and related functions here.(some functions require administrator privileges)
Save
Cancel
Logout
DOS ATTACK PROTECTION SETTINGS
Select DoS Attack protection settings Do according settings.
DoS Attack protection settings
Enable
Disable
SET FIREWALL LEVEL
SelectFirewall Level, Do according settings.

To set the basic firewall settings:

1. Under Set Firewall Level, select **Enable** or **Disable** to enable or disable the

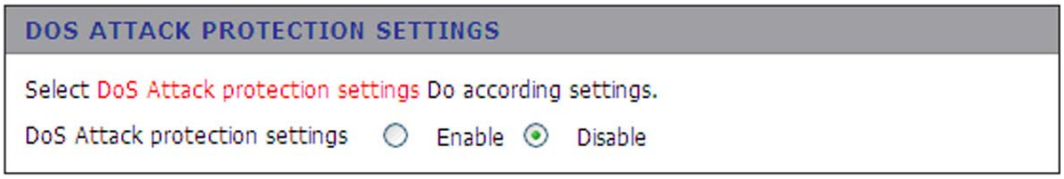
firewall feature,then set the firewall level as appropriate



2. Click **Save** to commit the changes.

To edit the DOS attack protection settings:

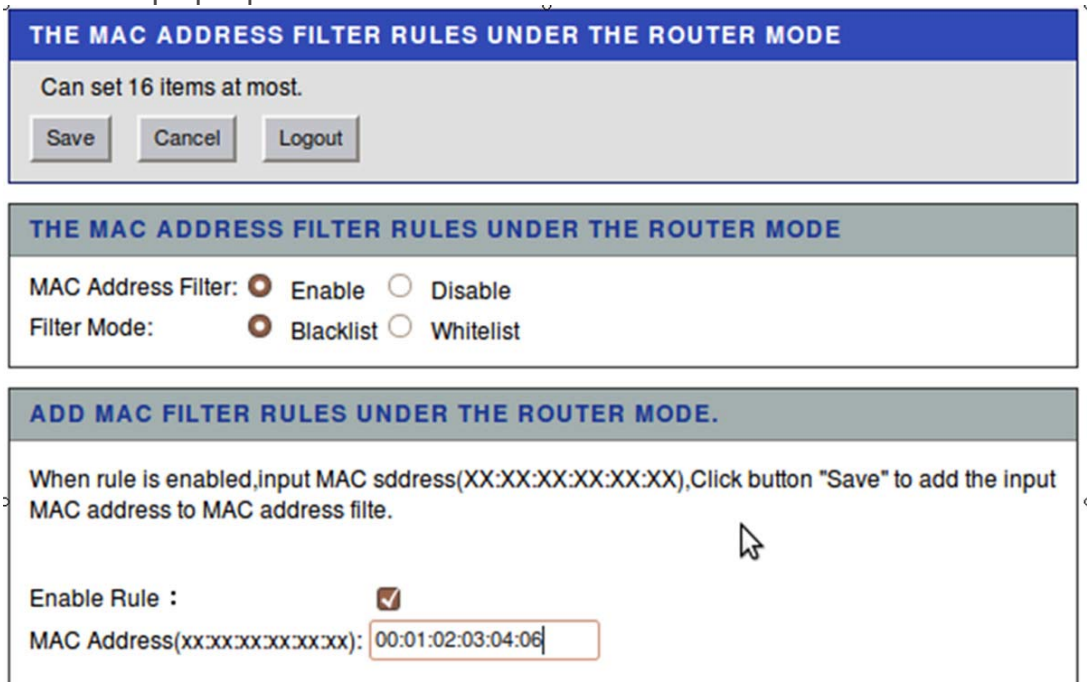
1. Under DOS Attack Protection Settings, select **Enable** or **Disable** to enable or disable the DOS
attack protection feature.


DOS ATTACK PROTECTION SETTINGS
Select DoS Attack protection settings Do according settings.
DoS Attack protection settings Enable Disable

2. Click **Save** to commit the changes.

To add a MAC filter set:

1. In the MAC Address Filter Rules Under Router Mode, choose **Enable** then click **OK** in the pop-up window


THE MAC ADDRESS FILTER RULES UNDER THE ROUTER MODE
Can set 16 items at most.
Save
Cancel
Logout
THE MAC ADDRESS FILTER RULES UNDER THE ROUTER MODE
MAC Address Filter: Enable Disable
Filter Mode: Blacklist Whitelist
ADD MAC FILTER RULES UNDER THE ROUTER MODE.
When rule is enabled,input MAC sddress(XX:XX:XX:XX:XX:XX),Click button "Save" to add the input MAC address to MAC address filte.
Enable Rule :
MAC Address(xx:xx:xx:xx:xx:xx): 00:01:02:03:04:06

ALG allows customized NAT traversal filters to plug into the gateway to support the address and port translation for application later control/data protocols, such as H.323, real-time streaming protocol (RTSP), layer 2 tunneling protocol (L2TP), IP

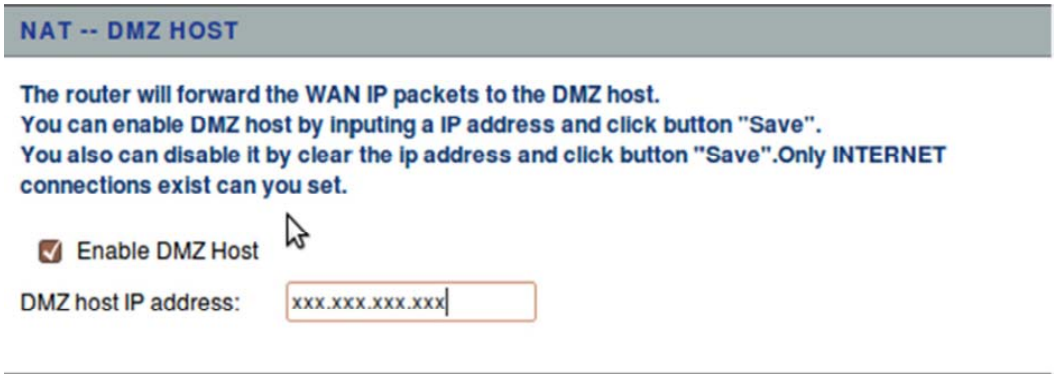
security (IPSEC), session initiation protocol (SIP).

To enable an ALG:

1. Check a specific ALG to enable it.
2. Click **Save** to commit the changes.

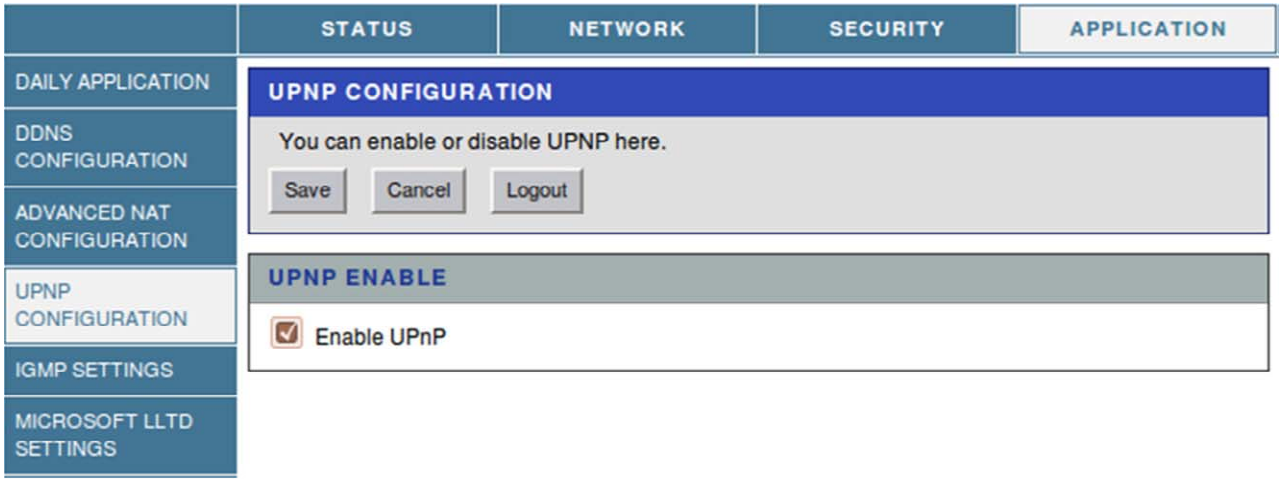
To enable a DMZ host:

Under NAT - DMZ Host, click Enable DMZ host and enter the DMZ host address.


NAT -- DMZ HOST
The router will forward the WAN IP packets to the DMZ host.
You can enable DMZ host by inputing a IP address and click button "Save".
You also can disable it by clear the ip address and click button "Save".Only INTERNET connections exist can you set.
Enable DMZ Host
DMZ host IP address:
xxx.xxx.xxx.xxx

3.2.15 UPnP (Router Build Only)

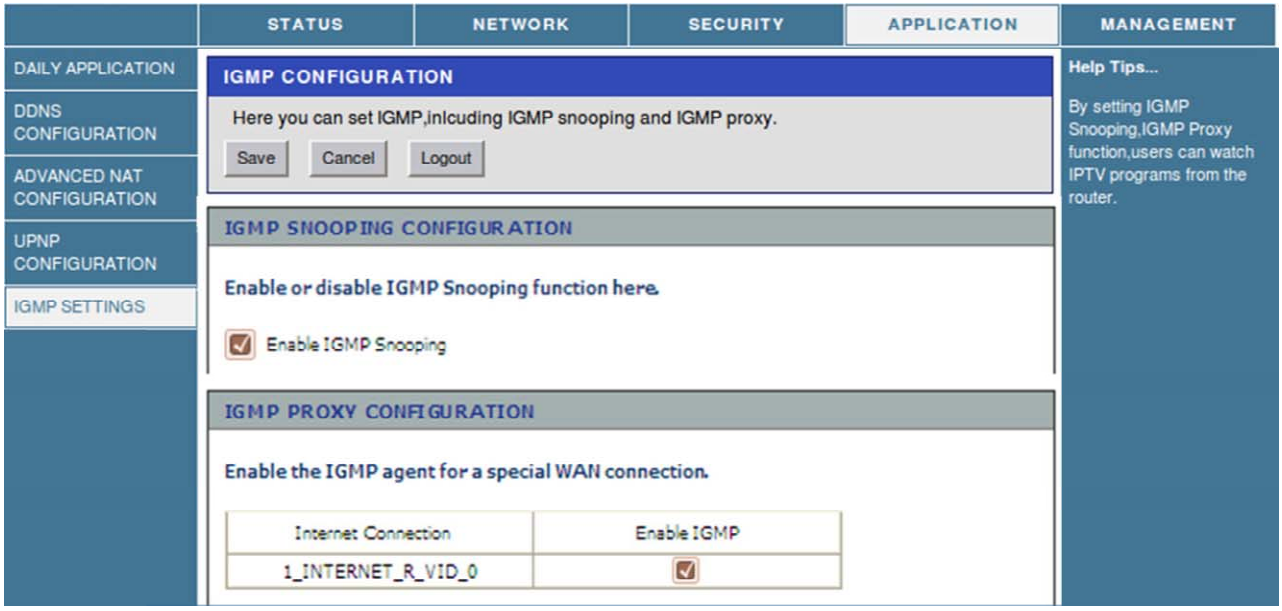
Click the **APPLICATION** tab and click **UPNP CONFIGURATION** to access the UPnP Settings screen.



1. Under UPnP Enable, check **Enable UPnP**.
2. Click **Save** to commit the changes.

3.2.16 IGMP Snooping (Router Build Only)

Click the **APPLICATION** tab and click **IGMP CONFIGURATION** to access the IGMP Settings screen.

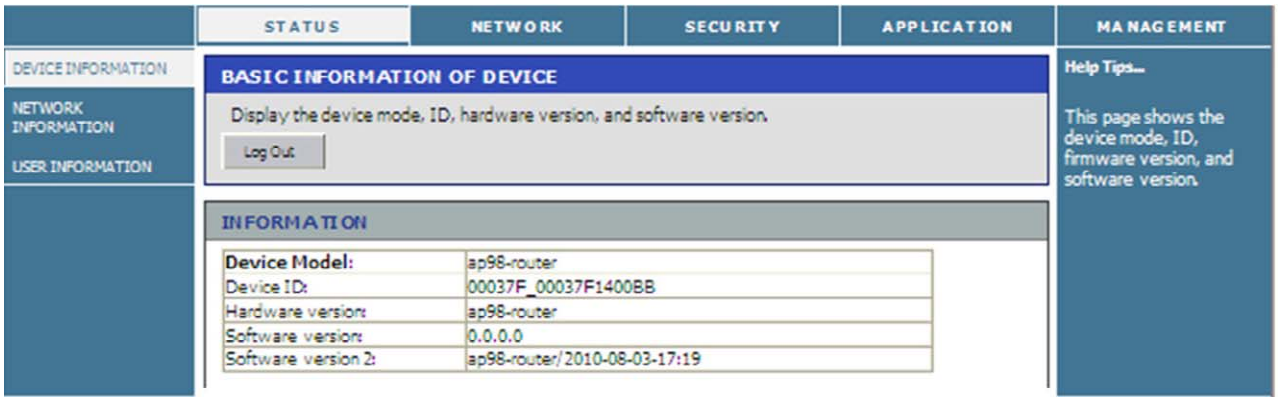


1. IGMP snooping requires an existing Internet connection. Check **Enable IGMP**.
2. Click **Save** to commit the changes.

Status Information

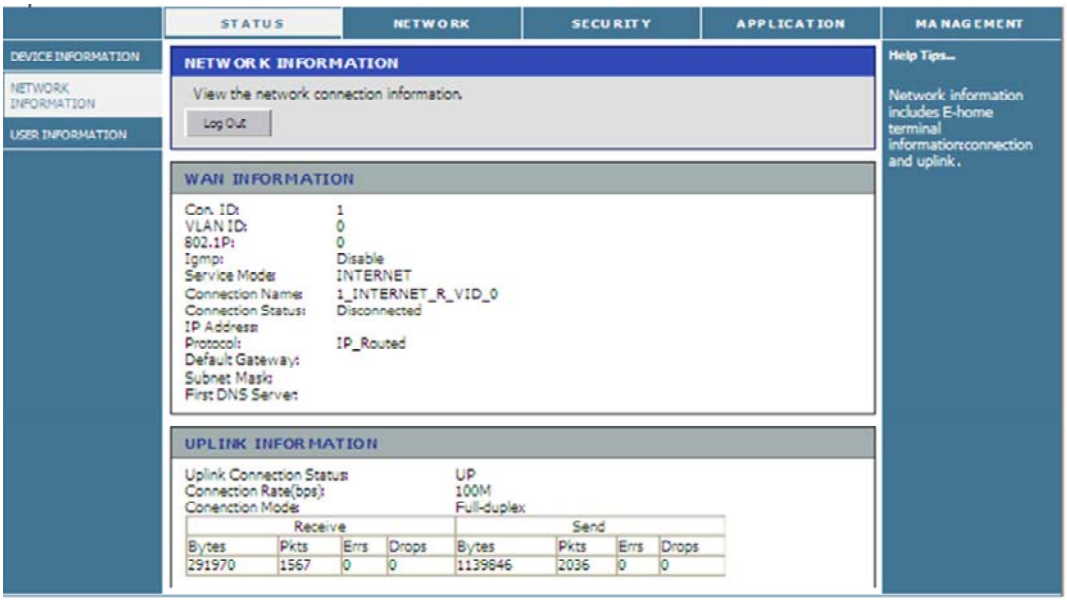
1 Device Information

Click the **STATUS** tab to show the basic device information, including the Device Model/ID and the hardware/software version.



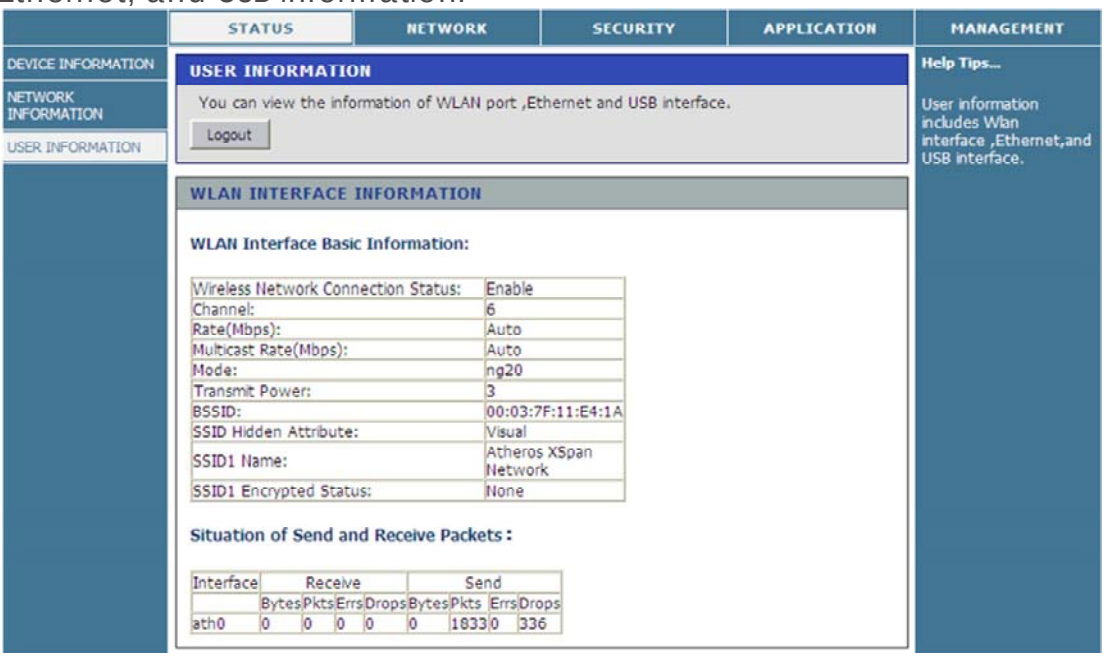
2 Network Status

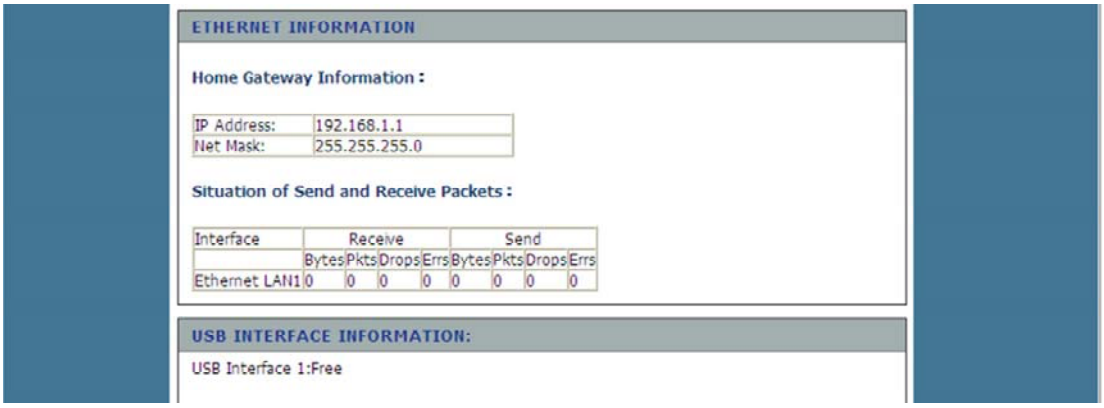
Click the **STATUS** tab and choose **NETWORK INFORMATION** to show the network-related information.



3 Wireless/Ethernet/USB Information

Click the **STATUS** tab and choose **USER INFORMATION** to show the LAN-side, Ethernet, and USB information.

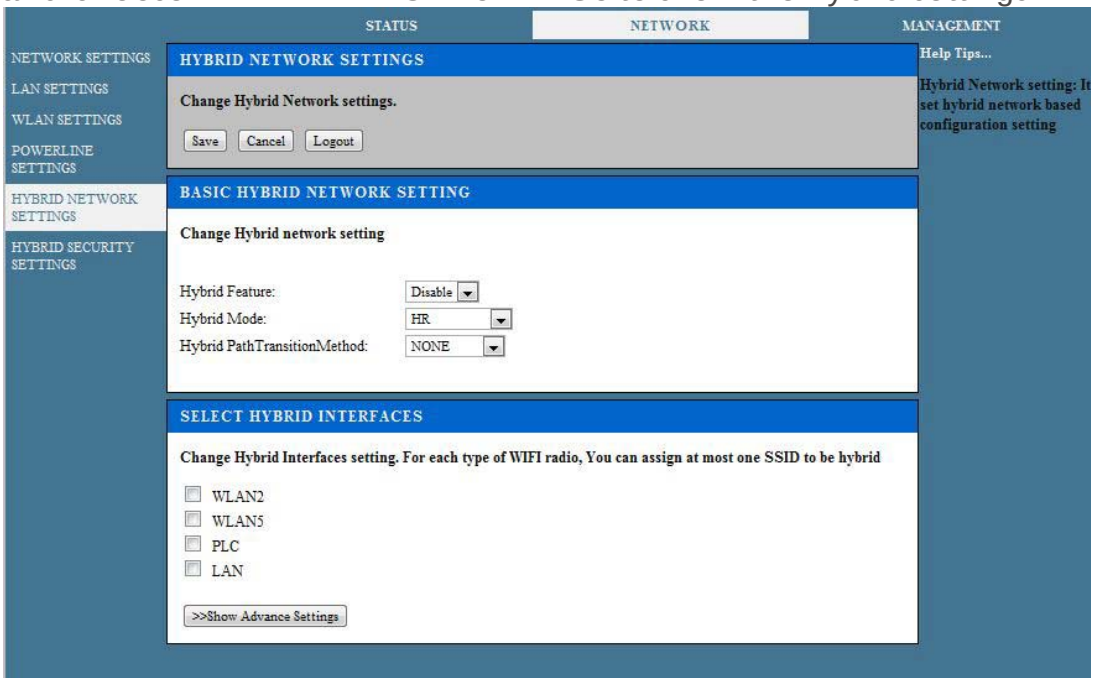



ETHERNET INFORMATION
Home Gateway Information :
IP Address: 192.168.1.1
Net Mask: 255.255.255.0
Situation of Send and Receive Packets :
Interface Receive Send
Bytes Pkts Drops Errs Bytes Pkts Drops Errs
Ethernet LAN1 0 0 0 0 0 0 0 0
USB INTERFACE INFORMATION:
USB Interface 1:Free

4 Hybrid Network Setting (APH126 Only)

Hybrid networking involves effective use of both wired and wireless technologies to provide seamless connectivity solutions that offer end-users a flexibility and performance within the home.

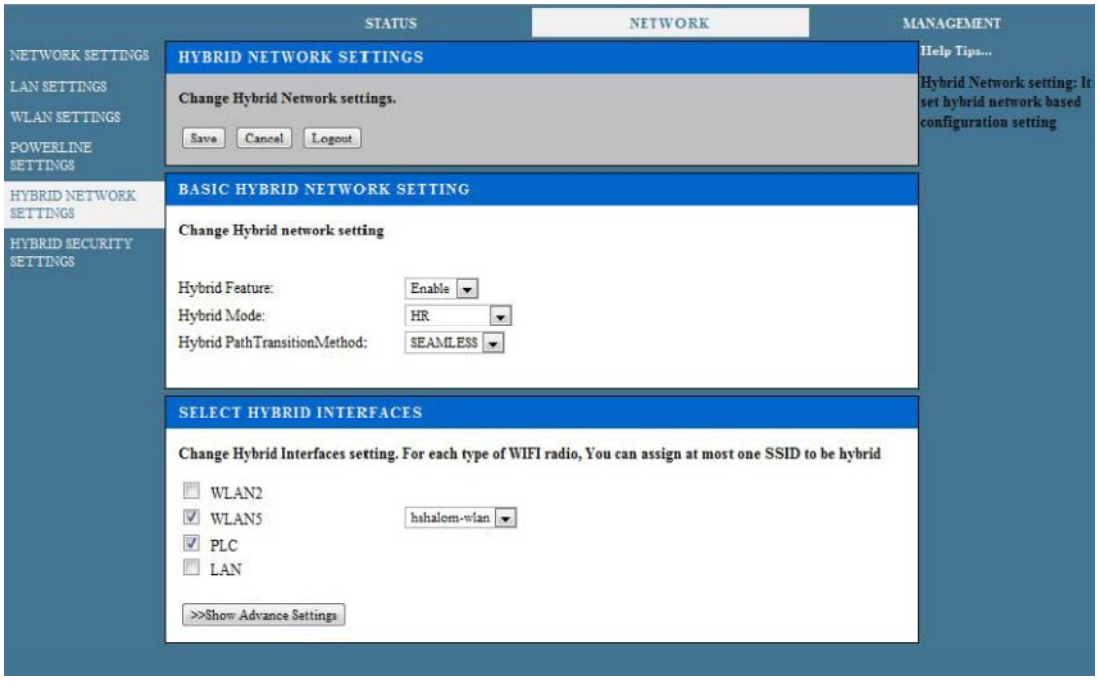
For carriers and retailers, hybrid solutions deliver more reliability and fewer customer service calls. To set up a hybrid networks build, choose the **NETWORK** tab and choose HYBRID NETWORK SETTINGS to show the hybrid settings.



5 Basic Hybrid Network Settings

The basic setting includes hybrid network mode and hybrid interface.

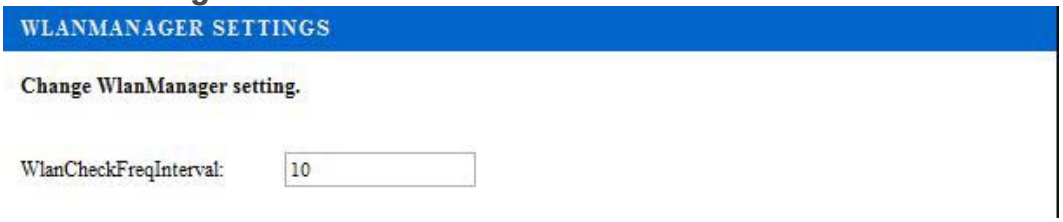
1. Under Hybrid Feature, select **Enable** from the drop-down menu.



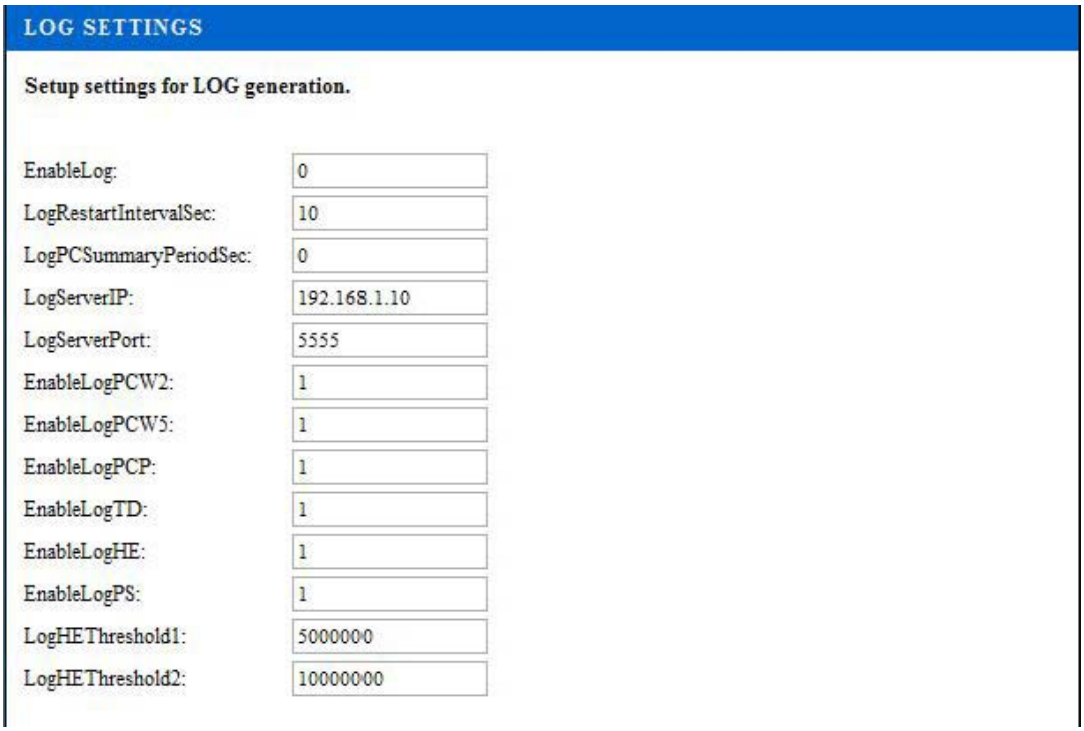
2. Under Hybrid Path Transmition Method drop-down menu, select “None” for default mode, select “SEAMLESS” for seamless path switching.
3. Select the hybrid interfaces WiFi interface setting. Note that for the WIFI interface, only one SSID can be set for each radio.
   WLAN2 (2.4 GHz)
   WLAN 5 (5 GHZ)
   PLC (Powerline interface)
   LAN (Ethernet interface)
   Click **Save**.

Path Selection

WLAN Manager



LOG



Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalency Privacy (WEP) offer different levels of security for wireless communication.

A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. And WPA2 is more secure than WPA. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment.

WEP is an older encryption standard and may be the only option available on some older devices that do not support WPA.

Note: Not all wireless adapter configuration utilities support WPA/WPA2. Furthermore, client software is required on the client. Windows XP with Service Pack 3, Windows 2000 with Service Pack 4, and Windows Vista include the client software that supports WPA/WPA2. Nevertheless, the wireless adapter hardware and driver must also support WPA/WPA2.

The PL9571-WAP provides the following levels of security: Open, WEP, WPA-Personal, WPA-Enterprise, WPA2-Personal and WPA2-Enterprise.

Table9-1: Wireless Security Options:

Field	Description
Open	No wireless security enabled.
WEP	WEP offers the following options: • **Open System** With Open Network Authentication and 64- or 128-bit WEP data encryption, the PL9571-WAP does perform 64- or 128-bit data encryption but does not perform any authentication • **Shared Key** Shared Key authentication encrypts the SSID and data. Choose the encryption strength (64- or 128-bit data encryption). Manually enter the key values which are case sensitive
WPA-Personal / WPA2-Personal	WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, TKIP or AES. (AES is a stronger encryption method than TKIP.) **WPA-Pre-Shared Key** (PSK) performs authentication, dynamically changes the encryption keys, making it nearly impossible to circumvent. **Group Key Renewal** is the Key Renewal period, which tells the Router how often it should change the encryption keys. The default Group Key Renewal period is 3600 seconds.
WPA- Enterprise / WPA2-Enterprise	This option features WPA used in coordination with Auth Server (This should only be used when a Auth server is connected to the PL9571.) The Auth Server IP, Port, and Secret (pass code) need to be configured in this mode.
802.1x	This option features 802.1xused in coordination with Auth Server (This should only be used when a Auth server is connected to the PL9571.) The Auth Server IP, Port, and Secret (pass code) need to be configured in this mode.

The following note applies to WEP Security Type:
ASCII-Any combination of letters and numbers
5 Characters (64Bit) / 13 Characters (128 Bit)
HEX – Any combination of numbers (0-9) and letters (A-F)
10 Characters (64 Bit) / 26 Characters (128 Bit)

Configuring Wireless Security

By default, the PL9571-WPA security options are enabled. The default security type is set to WPA2-Personal AES; and its security key is the last 10 digits of the PL9571's serial number shown on the label. The security options should be configured by advanced users only. To change the security option, follow the steps bellow.

1. Click on Network from the top main menu.
2. Click on Wireless Settings from the Sub Navigation Link. The security dialog page will appear.
3. Make your selection under *Security Type* from the drop down list.
4. Fill in the gaps according to your Security Type selection.
5. Enter your new security key (PSK for WPA2-Personal Security Type).
6. Click Save
7. You are done.

How the NID and WPS-Push Button can be used

Following is an example of how the **NID** button can be used:

1. Select a PlugLink 9571 device in your network. Press and hold the **NID** button for 10 seconds. After about 10 seconds, the lights on your device will blink off briefly and come back on immediately. This will change the existing Network Encryption Key (NEK) to a randomized NEK.
2. On the PlugLink 9571 device from Step #1, press and hold the **NID** button for about 2 seconds. The power light on the device will begin flashing. This unit has now been set to allow other units to join the network and be assigned the same password. This unit will remain in "adder" mode for about 2 minutes.
3. Before the three minutes is up from Step #2, select another PlugLink device from your network. Press and hold the **NID** button for about 2 seconds. The power light on the device will blink as well. The two devices will communicate and the second device will have its NEK set to the NEK of the first device. This should happen in about 15 to 20 seconds. Once the process has been completed, you can then test if the two devices are communicating.

4. If you add units at a later time, you only need to perform Step #2 (using any device in the network) and Step #3 (any new devices). Step #1 is not necessary unless you wish to change your NEK.

Following is a basic description of how the **WPS-Push Button** can be used:

1. Press **WPS**/sw2 for more than 5 seconds. (Or click Reset WPS network button on the web interface's wireless-basic-settings tab). This will create a new wireless network with random SSID, random wireless password and WPA2-Personal-AES security algorithm. The PL9571 will wait 2 minutes for a client to join the wireless network by pushing the client's **WPS** button.

2. Press **WPS**/sw2 for less than 5 seconds (or click **WPS AP** Push Button on the web interface's wireless-basic-settings tab).

a) If the current wireless network was not created by WPS:

Pressing the WPS/sw2 button will create a new wireless network with a random SSID, random wireless password using the WPA2-Personal-AES security algorithm. After the new wireless network is created, the PL9571 will wait 2 minutes for a client to join the wireless network by pushing the client's WPS button.

b) If the current wireless network was created by WPS:

The PL9571 will use the current SSID/wireless password and retain the current clients' connections in the wireless network. The PL9571 will wait
2 minutes for any new clients to join the wireless network by pushing the client's WPS button.

The SSID and wireless password can be checked from web interface's wireless-status tab. Users can also use this information and manually connect to the wireless network.

3. If you have multiple clients that wish to join the wireless network, you will have to press the WPS/sw2 button for 5 seconds (or less) for every client. The user will then have to press the WPS button to join the network.

Following is an example to make your network:

1. Press and hold the **SW2** (Right) button for more than 10 seconds. This will reset the current wireless network and create a new wireless network with random SSID, random wireless password and WPA2-Personal-AES security algorithm. The PL9571 will wait 2 minutes for a client to join the wireless network by pushing the client's **WPS** button.
2. Before the 2 minutes have elapsed, push a client's **WPS** button. The client will join the network created at Step 1.
3. If there are additional clients that wish to join the WPS network, push the **SW2** (Right) button for less than 3 seconds and push a client's **WPS** button, this will add one connection. Repeat for every client that needs to join the WPS network.
4. For clients without **WPS** push button capabilities, you can make a manual connection using the WPA2-Personal-AES security algorithm and inputting the SSID and wireless password information which is available from the web-interface's wireless-status tab.

Chapter 9

Technical Support

PLEASE REFER TO THE WARRANTY AND SUPPORT INFORMATION CARD THAT WAS SHIPPED WITH YOUR PRODUCT.

By registering your product at www.asokatech.com/register, we can provide you with faster expert technical support and timely notices of product and software upgrades.

Support Information
Phone: 1-408-550-8167
Email: support@asokatech.com
URL: www.asokatech.com

Chapter 10

Technical Specifications

Standards Compliance
- HomePlug® AV
- IEEE 1901, IEEE 802.3,
- IEEE 802.11b/g/n

System Requirements
- Windows® 98, 2000, XP , Vista
- and Windows 7

Network Protocol
- TCP/IP, IEEE 802.3 Ethernet,
- IEEE 802.11b/g
- IEEE 802.1x

Network Interface
- Two 10/100 Base-T Ethernet (RJ-45)
- HomePlug® AV PowerLine 1.0
- 802.11b/g /n
-

Bandwidth
- PLC 500 Mbps

Operating Frequency
- 2 to 70 MHz over Powerline
- 2.4GHz over wireless

Modulation Schemes
- Orthogonal Frequency Division Multiplexing (OFDM)
- QAM4096/1024/256/64/16
- QPSK
- BPSK

Wireless Security
- WEP, WPA, WPA2,802.1x

Distance
- Up to 328 feet (100 Meters) over wireless
- Up to 1000 feet (300 Meters) over powerline

Quality of Service (QoS)
- TOS
- 802.1q

Additional Protocols
- Forward Error Correction (FEC)
- Automatic Channel Adaptation

Power Supply
- US Version: 100-120VAC
- UK/EU Version: 220-240VAC

Power Rating
- US Version: 100-120VAC 0.25A, 60Hz
- UK/EU Version: 220-240VAC 0.15A, 50Hz

LEDs
- Power
- PLC Activity
- Wireless
- Ethernet Activity

Dimensions
- Size: (L104 x W66 x H31mm)
- Weight: 136g

Environmental Specifications
- Operating temperature: 32°F to 113°F (0°C to 45°C)
- Operating humidity: 10% to 85% Non-Condensing
- Storage temperature: -4°F to 185°F (-20°C to 80°C)
- Storage humidity: 5% to 90% Non-Condensing

Electromagnetic Emissions/EMI Safety
- FCC Part 15 Class B
- UL (US and Canada)
- CE

Surge Protection
- 4KV/6KV

Warranty
- 1-year limited

Chapter 11

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and
(2) This device must accept any interference received, including interference that may cause undesired operation.

FCC RF Radiation Exposure Statement:

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

Chapter 12

Warranty Information

Asoka warrants that (a) the hardware components of the product will be free from defects in materials and workmanship under normal use for one (1) year from the date of purchase when used within the limits set forth in the Specifications section of the User Guide, and (b) the software components will perform substantially in accordance with Asoka's published specifications for ninety (90) days from the date of purchase, but does not warrant that the software will be error-free or free of all defects.

Should a product fail to perform as described in the User Guide, it will be repaired or replaced with the same or functionally equivalent product by Asoka, at its discretion, free of charge provided that you: (a) return the failed product to an Asoka designated repair facility with shipping charge prepaid, and (b) provide Asoka with proof of the original date of purchase. Repaired or replacement products will be returned to you with shipping charges prepaid. Asoka warrants any replaced or repaired product or component for the life of the product.

This warranty extends only to you, the original purchaser and is not transferable to any subsequent purchasers.

This warranty does not apply if, in the judgment of Asoka, the product fails due to damage from shipment, handling, storage, accident, abuse, misapplication or misuse, or if it has been used or maintained in a manner not conforming to product manual instructions, has been modified in any way, or has had any serial number removed or defaced. Repair by anyone other than Asoka or an approved agent will void this warranty. The maximum liability of Asoka under this warranty is limited to the purchase price of the product covered by the warranty. Prior to returning any defective product, the purchaser or the authorized merchant from whom the purchaser originally bought the product must obtain a Return Material Authorization (RMA) number from Asoka. All defective products should be returned to Asoka with shipping charges prepaid. Asoka will not accept collect shipments.

WHILE ASOKA HAS MADE EVERY EFFORT TO PROVIDE CLEAR AND ACCURATE TECHNICAL INFORMATION ABOUT ITS PRODUCTS, ASOKA ASSUMES NO LIABILITY FOR ANY EVENTS ARISING OUT OF THE USE OF THE TECHNICAL INFORMATION OR THE PRODUCT. EXCEPT AS SPECIFICALLY PROVIDED IN THIS AGREEMENT OR AS REQUIRED BY LAW, THE WARRANTIES AND REMEDIES STATED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHERS, ORAL OR WRITTEN, EXPRESS OR IMPLIED. ANY AND ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS ARE EXPRESSLY EXCLUDED. NEITHER ASOKA NOR BELLSOUTH SHALL BE LIABLE, UNDER ANY CIRCUMSTANCES, TO ANY PERSON OR ENTITYFOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, DAMAGES RESULTING FROM THE USE OR MALFUNCTION OF THE PRODUCTS, LOSS OF PROFITS OR REVENUES, BUSINESS INTERRUPTION, OR COSTS OF REPLACEMENT GOODS, EVEN IF ASOKA OR BELLSOUTH IS INFORMED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

Asoka USA Corporation
2620 Augustine Drive Suite 230
230 Santa Clara, California 95054
USA Phone: (408) 550–8167
Fax: (408) 884–2390
www.asokatech.com

66-0377-01Rev.001